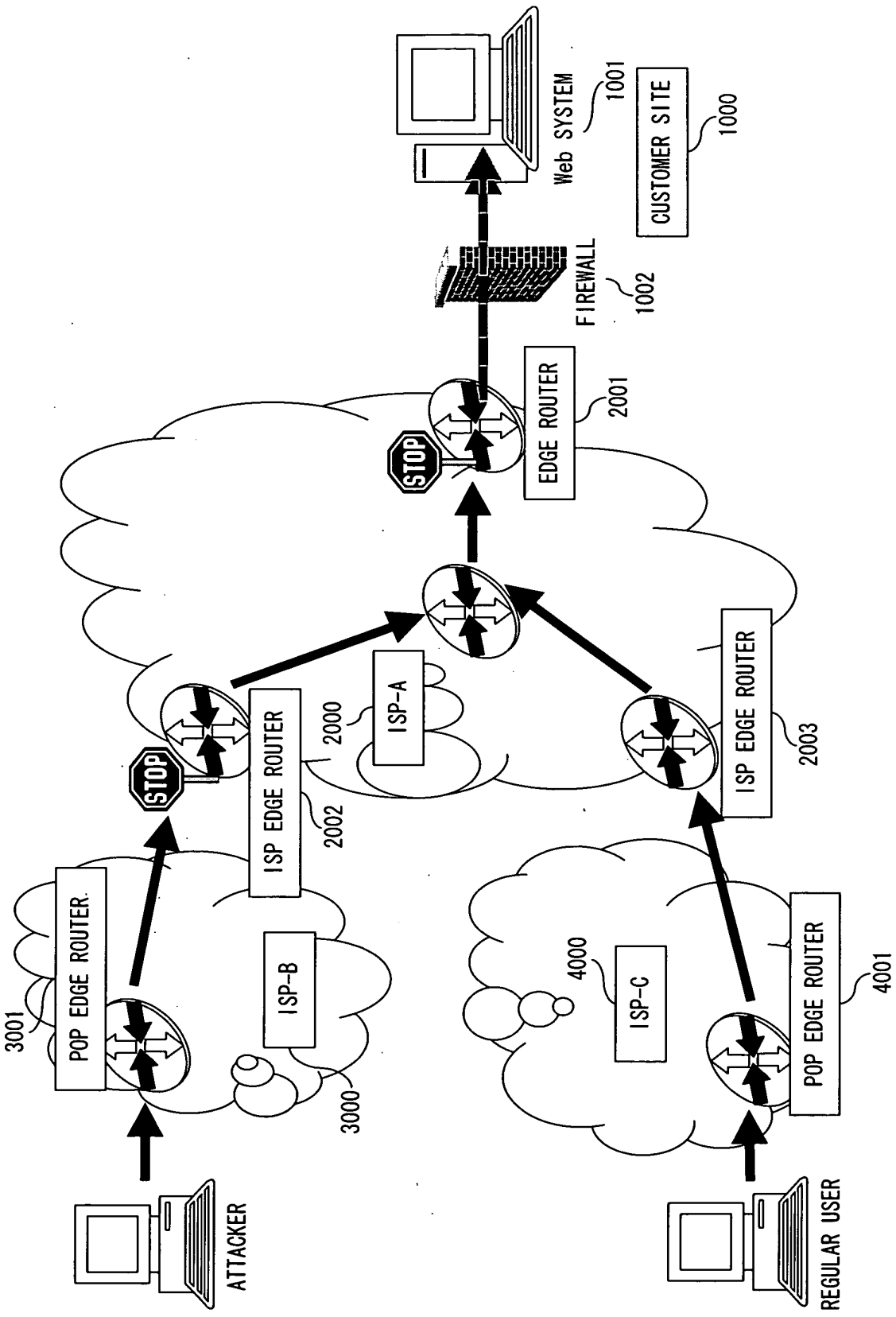

FIG. 1

PRIOR ART

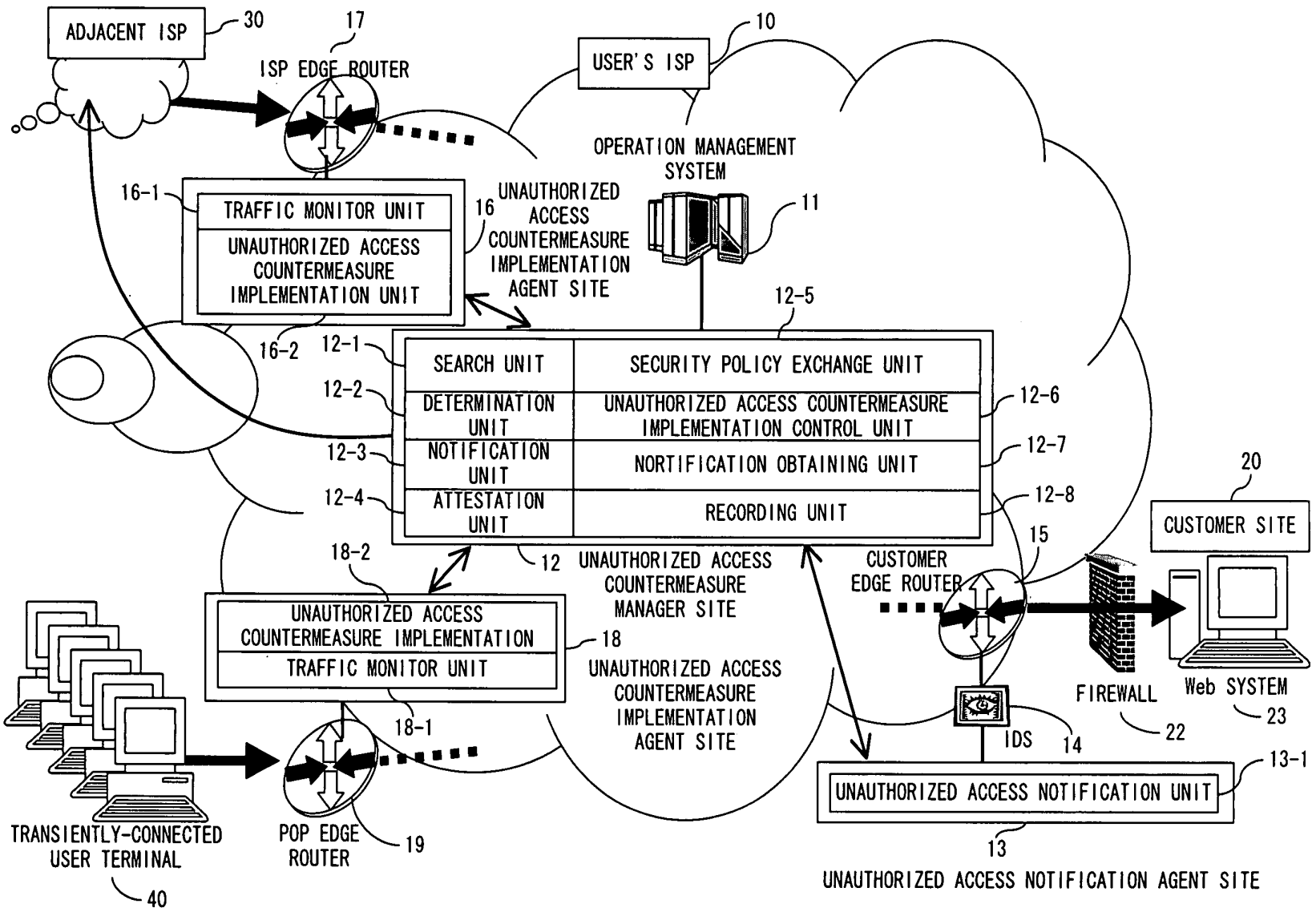

FIG. 2

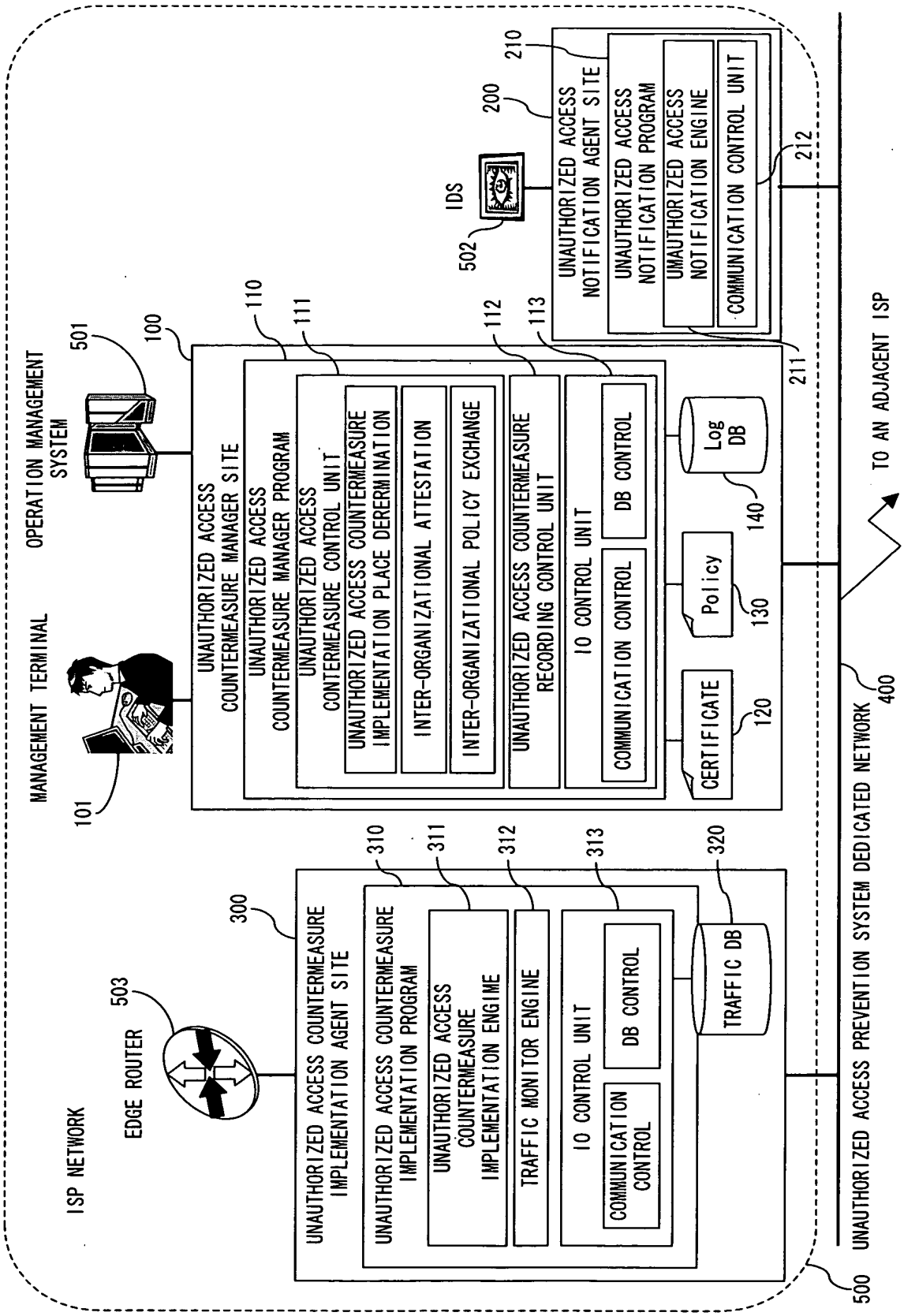
ISP NETWORK
EDGE ROUTER
503
300
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION AGENT SITE
310
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION PROGRAM
311
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION ENGINE
312
TRAFFIC MONITOR ENGINE
313
IO CONTROL UNIT
COMMUNICATION CONTROL
DB CONTROL
320
TRAFFIC DB
500
UNAUTHORIZED ACCESS PREVENTION SYSTEM DEDICATED NETWORK
400
TO AN ADJACENT ISP
MANAGEMENT TERMINAL
101
OPERATION MANAGEMENT SYSTEM
501
100
UNAUTHORIZED ACCESS COUNTERMEASURE MANAGER SITE
110
UNAUTHORIZED ACCESS COUNTERMEASURE MANAGER PROGRAM
111
UNAUTHORIZED ACCESS CONTERMEASURE CONTROL UNIT
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION PLACE DERERMINATION
INTER-ORGANIZATIONAL ATTESTATION
INTER-ORGANIZATIONAL POLICY EXCHANGE
112
UNAUTHORIZED ACCESS COUNTERMEASURE RECORDING CONTROL UNIT
113
IO CONTROL UNIT
COMMUNICATION CONTROL
DB CONTROL
CERTIFICATE
120
Policy
130
Log DB
140
211
212
IDS
502
200
210
UNAUTHORIZED ACCESS NOTIFICATION AGENT SITE
UNAUTHORIZED ACCESS NOTIFICATION PROGRAM
UNAUTHORIZED ACCESS NOTIFICATION ENGINE
COMMUNICATION CONTROL UNIT

FIG. 3

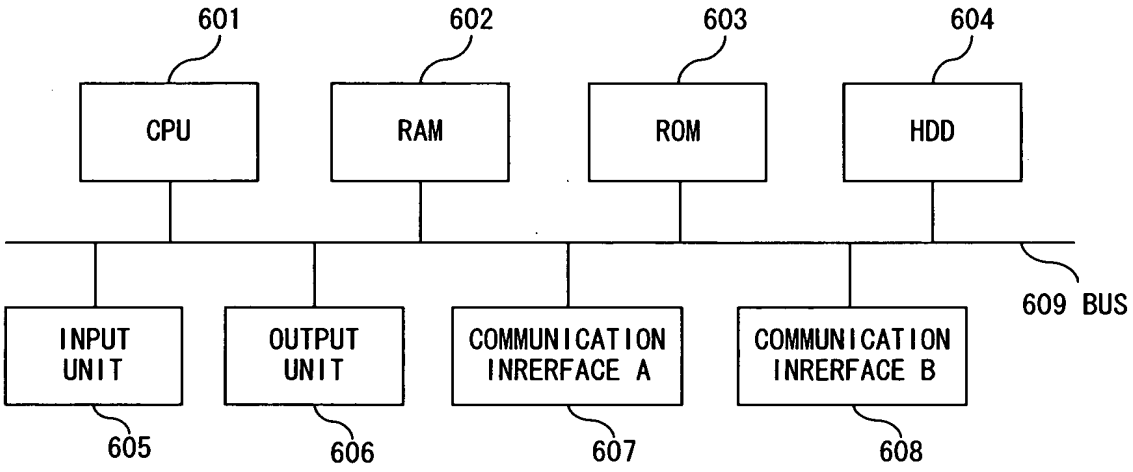
601
602
603
604
CPU
RAM
ROM
HDD
609 BUS
INPUT UNIT
OUTPUT UNIT
COMMUNICATION INRERFACE A
COMMUNICATION INRERFACE B
605
606
607
608

FIG. 4

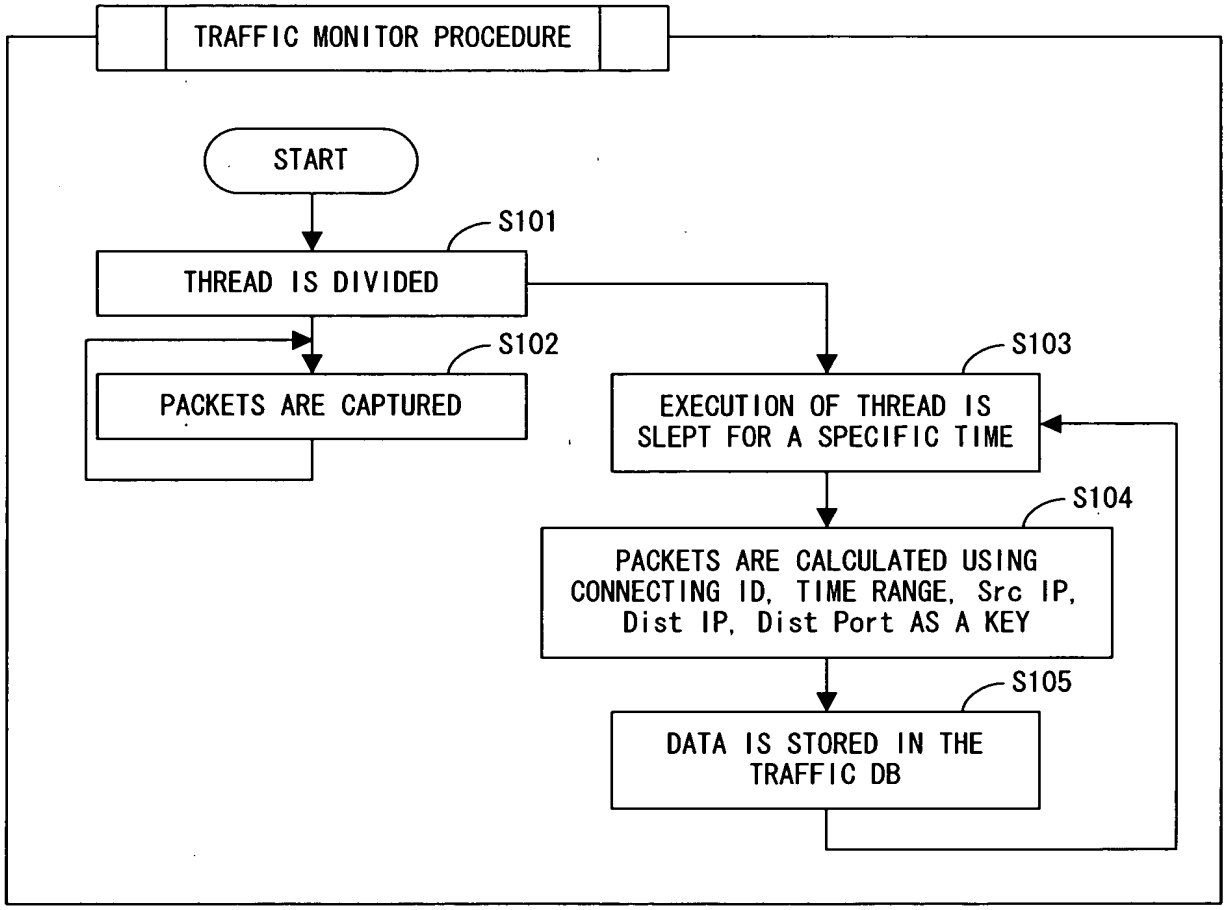
TRAFFIC MONITOR PROCEDURE
START
S101
THREAD IS DIVIDED
S102
PACKETS ARE CAPTURED
S103
EXECUTION OF THREAD IS SLEPT FOR A SPECIFIC TIME
S104
PACKETS ARE CALCULATED USING CONNECTING ID, TIME RANGE, Src IP, Dist IP, Dist Port AS A KEY
S105
DATA IS STORED IN THE TRAFFIC DB

FIG. 5

CONNECTING ID	TIME RANGE	Src IP	Dist IP	Dist Port	Count
ABC01234	10:00-10:10	202.248.20.254	202.248.20.68	80	1456
NBC56780	10:00-10:10	202.248.20.112	202.248.20.68	80	35724
AS245	10:00-10:10	10.34.195.194	202.248.20.68	80	169043

FIG. 6

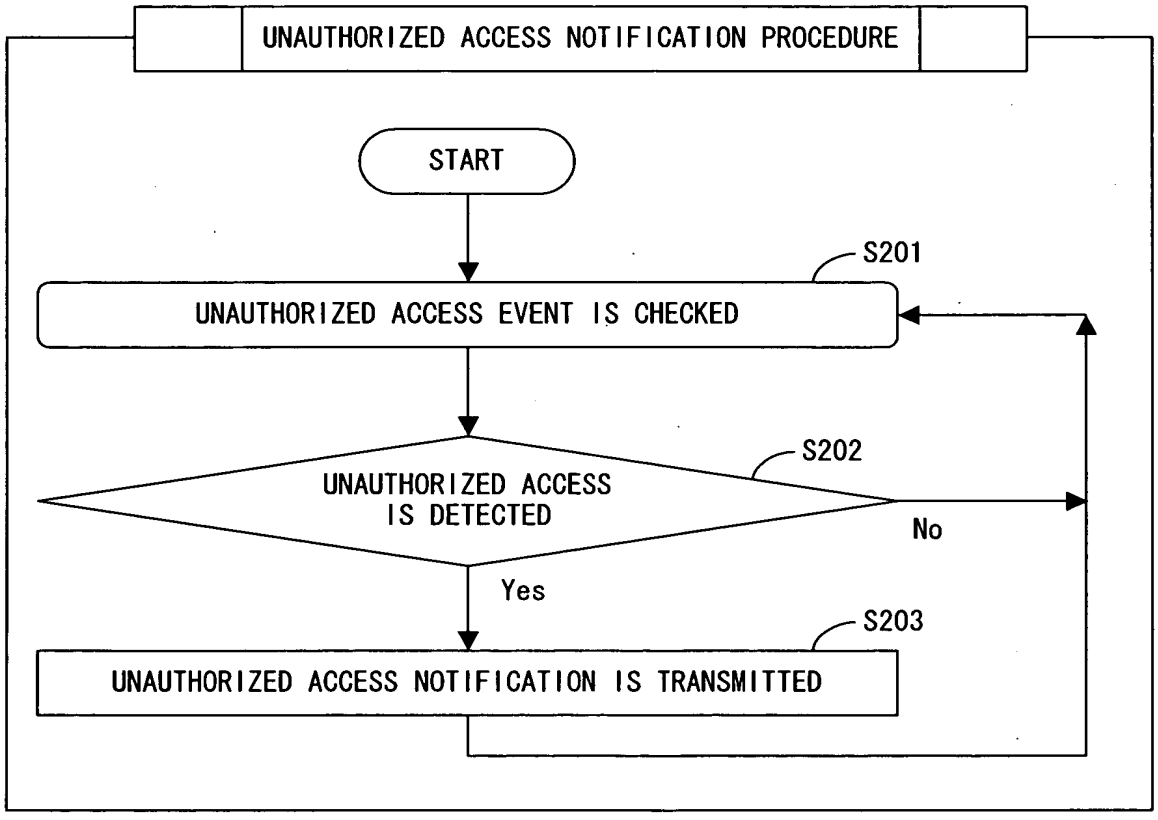
UNAUTHORIZED ACCESS NOTIFICATION PROCEDURE
START
S201
UNAUTHORIZED ACCESS EVENT IS CHECKED
S202
UNAUTHORIZED ACCESS IS DETECTED
No
Yes
S203
UNAUTHORIZED ACCESS NOTIFICATION IS TRANSMITTED

FIG. 7

DATA MEMBER	EXAMPLE 1	EXAMPLE 2
DETECTING ID	00-00-0E-82-2E-74-0001	00-00-0E-82-2E-74-0002
TIME RANGE START (GMT)	2003/2/1 16:01:16	2003/2/17 11:31:11
TIME RANGE END (GMT)	2003/2/1 16:11:16	2003/2/17 11:41:11
ATTACK CATEGORY	TCP Syn Flood	Worm
ORGANIZATION NAME	Company A	Company B
BELONGING ISP	ISP ABC	ISP XYZ
TARGET PROTOCOL	TCP	UDP
Src IP	10.4.120.Z	169.0.255.C
Dist IP	192.168.X.Y	164.71.A.B
Dist Port	80	1434
NUMBER OF UNAUTHORIZED PACKETS	156789	876534
ATTACK TOOL NAME	TFN2K	SQL Slammer
COUNTERMEASURE CANCELLATION POLICY	10 MINUTES	20 MIMUTES

FIG. 8

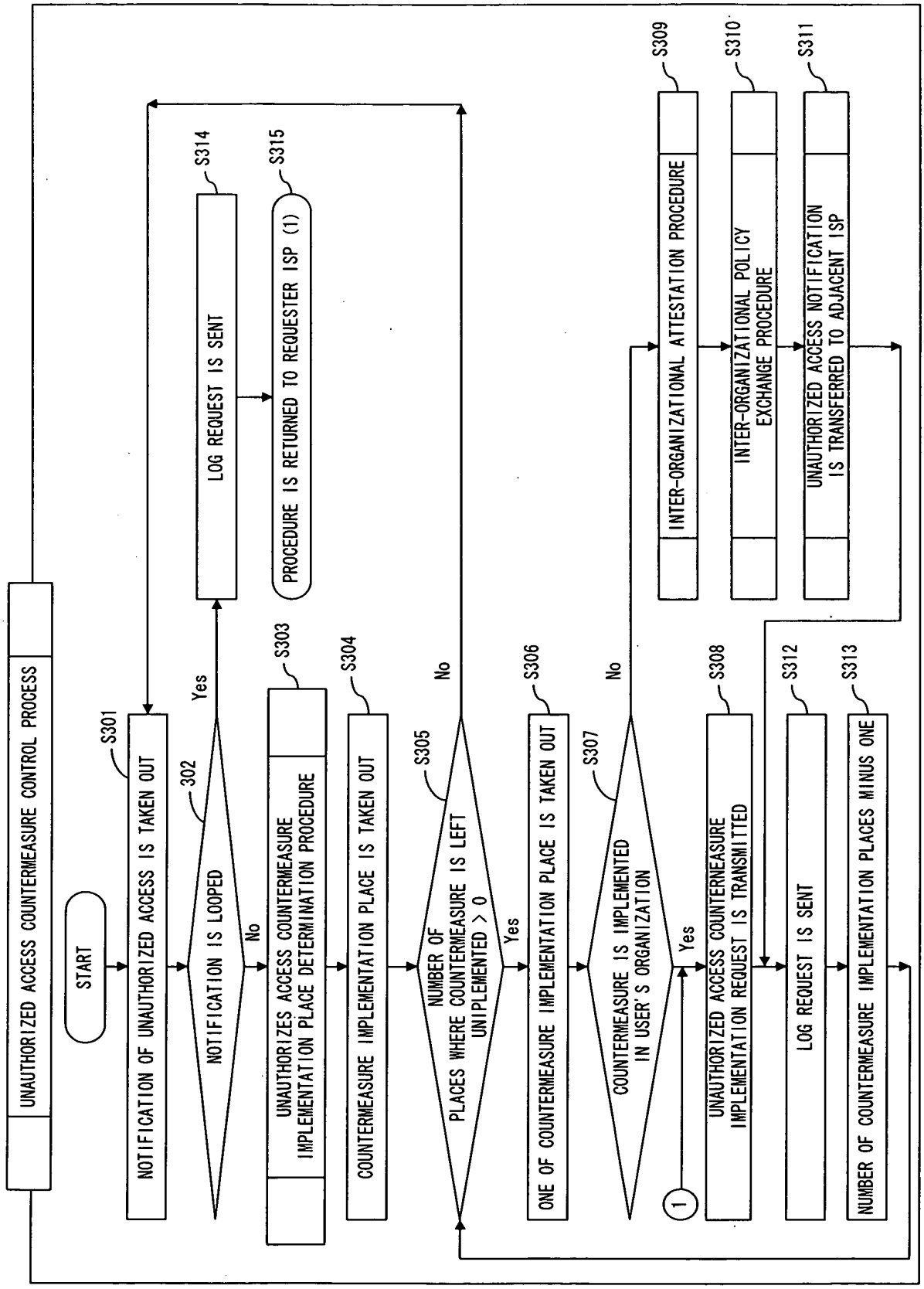
UNAUTHORIZED ACCESS COUNTERMEASURE CONTROL PROCESS
START
S301
NOTIFICATION OF UNAUTHORIZED ACCESS IS TAKEN OUT
302
NOTIFICATION IS LOOPED
Yes
No
S314
LOG REQUEST IS SENT
S315
PROCEDURE IS RETURNED TO REQUESTER ISP (1)
S303
UNAUTHORIZES ACCESS COUNTERMEASURE IMPLEMENTATION PLACE DETERMINATION PROCEDURE
S304
COUNTERMEASURE IMPLEMENTATION PLACE IS TAKEN OUT
S305
NUMBER OF PLACES WHERE COUNTERMEASURE IS LEFT UNIPLEMENTED > 0
No
Yes
S306
ONE OF COUNTERMEASURE IMPLEMENTATION PLACE IS TAKEN OUT
S307
COUNTERMEASURE IS IMPLEMENTED IN USER'S ORGANIZATION
No
Yes
1
S308
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION REQUEST IS TRANSMITTED
S312
LOG REQUEST IS SENT
S313
NUMBER OF COUNTERMEASURE IMPLEMENTATION PLACES MINUS ONE
S309
INTER-ORGANIZATIONAL ATTESTATION PROCEDURE
S310
INTER-ORGANIZATIONAL POLICY EXCHANGE PROCEDURE
S311
UNAUTHORIZED ACCESS NOTIFICATION IS TRANSFERRED TO ADJACENT ISP

FIG. 9

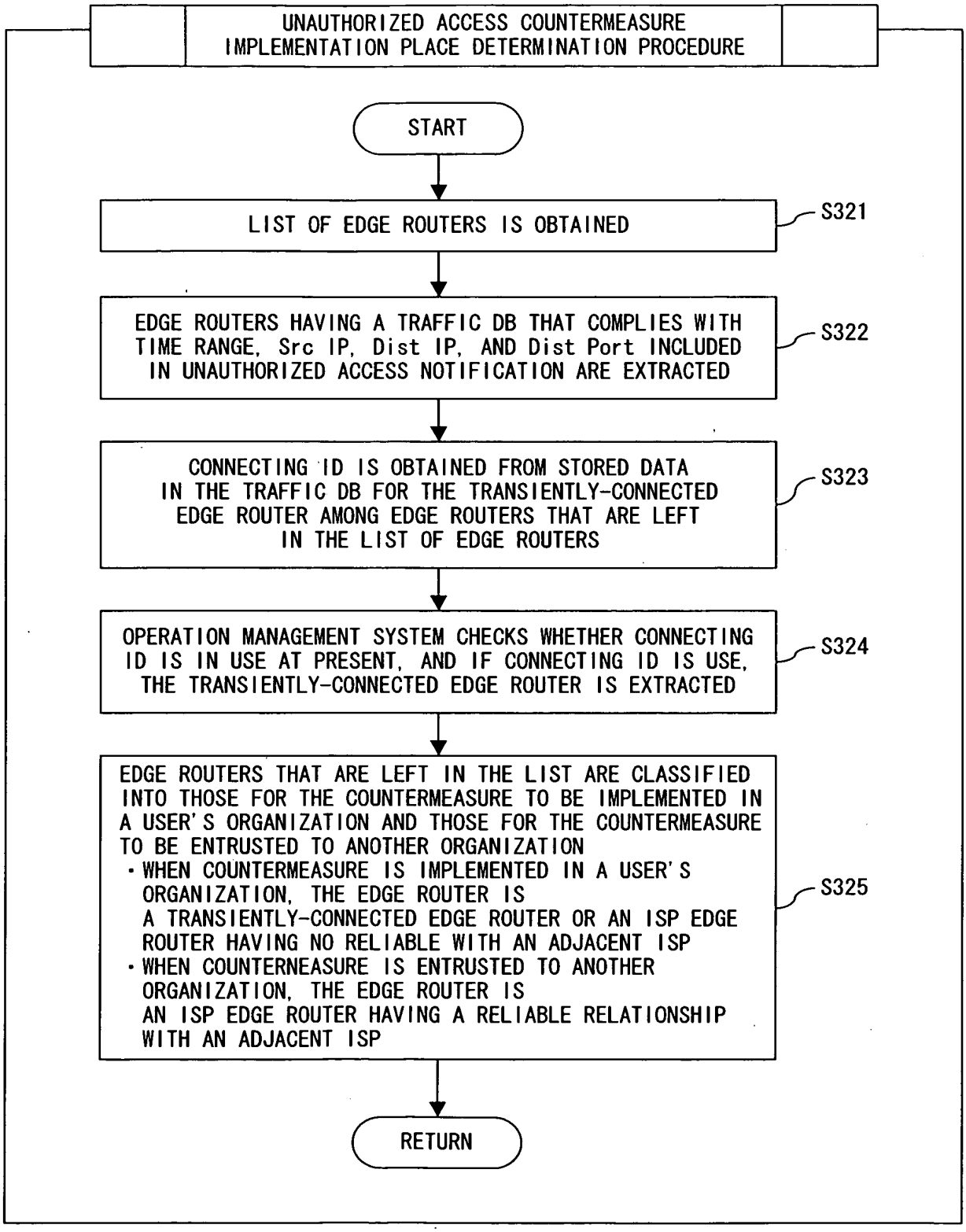
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION PLACE DETERMINATION PROCEDURE
START
LIST OF EDGE ROUTERS IS OBTAINED
S321
EDGE ROUTERS HAVING A TRAFFIC DB THAT COMPLIES WITH TIME RANGE, Src IP, Dist IP, AND Dist Port INCLUDED IN UNAUTHORIZED ACCESS NOTIFICATION ARE EXTRACTED
S322
CONNECTING ID IS OBTAINED FROM STORED DATA IN THE TRAFFIC DB FOR THE TRANSIENTLY-CONNECTED EDGE ROUTER AMONG EDGE ROUTERS THAT ARE LEFT IN THE LIST OF EDGE ROUTERS
S323
OPERATION MANAGEMENT SYSTEM CHECKS WHETHER CONNECTING ID IS IN USE AT PRESENT, AND IF CONNECTING ID IS USE, THE TRANSIENTLY-CONNECTED EDGE ROUTER IS EXTRACTED
S324
EDGE ROUTERS THAT ARE LEFT IN THE LIST ARE CLASSIFIED INTO THOSE FOR THE COUNTERMEASURE TO BE IMPLEMENTED IN A USER'S ORGANIZATION AND THOSE FOR THE COUNTERMEASURE TO BE ENTRUSTED TO ANOTHER ORGANIZATION
・WHEN COUNTERMEASURE IS IMPLEMENTED IN A USER'S ORGANIZATION, THE EDGE ROUTER IS A TRANSIENTLY-CONNECTED EDGE ROUTER OR AN ISP EDGE ROUTER HAVING NO RELIABLE WITH AN ADJACENT ISP
・WHEN COUNTERNEASURE IS ENTRUSTED TO ANOTHER ORGANIZATION, THE EDGE ROUTER IS AN ISP EDGE ROUTER HAVING A RELIABLE RELATIONSHIP WITH AN ADJACENT ISP
S325
RETURN

FIG. 10

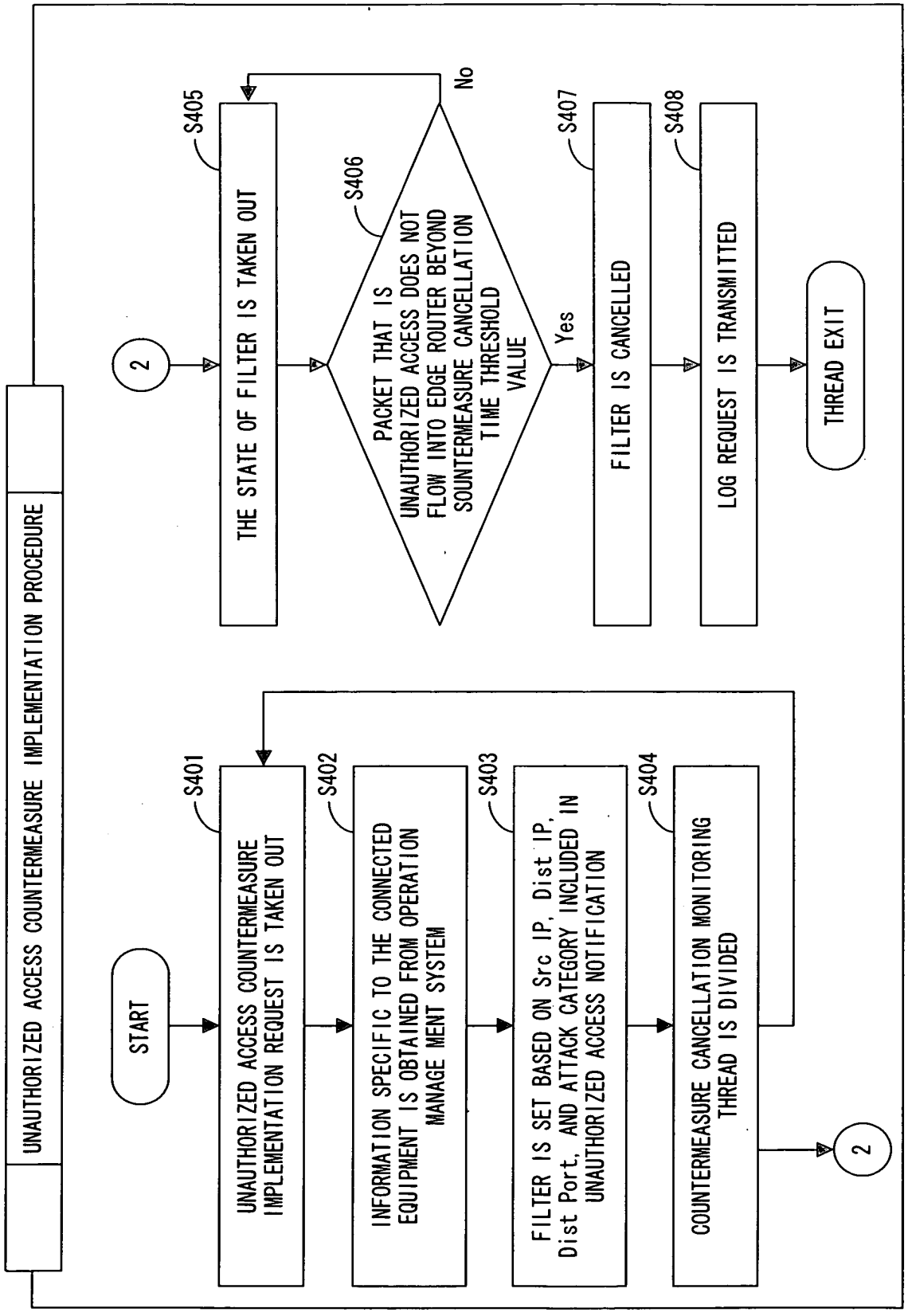
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION PROCEDURE
START
S401
UNAUTHORIZED ACCESS COUNTERMEASURE IMPLEMENTATION REQUEST IS TAKEN OUT
S402
INFORMATION SPECIFIC TO THE CONNECTED EQUIPMENT IS OBTAINED FROM OPERATION MANAGE MENT SYSTEM
S403
FILTER IS SET BASED ON Src IP, Dist IP, Dist Port, AND ATTACK CATEGORY INCLUDED IN UNAUTHORIZED ACCESS NOTIFICATION
S404
COUNTERMEASURE CANCELLATION MONITORING THREAD IS DIVIDED
2
2
S405
THE STATE OF FILTER IS TAKEN OUT
S406
PACKET THAT IS UNAUTHORIZED ACCESS DOES NOT FLOW INTO EDGE ROUTER BEYOND SOUNTERMEASURE CANCELLATION TIME THRESHOLD VALUE
No
Yes
S407
FILTER IS CANCELLED
S408
LOG REQUEST IS TRANSMITTED
THREAD EXIT

FIG. 11

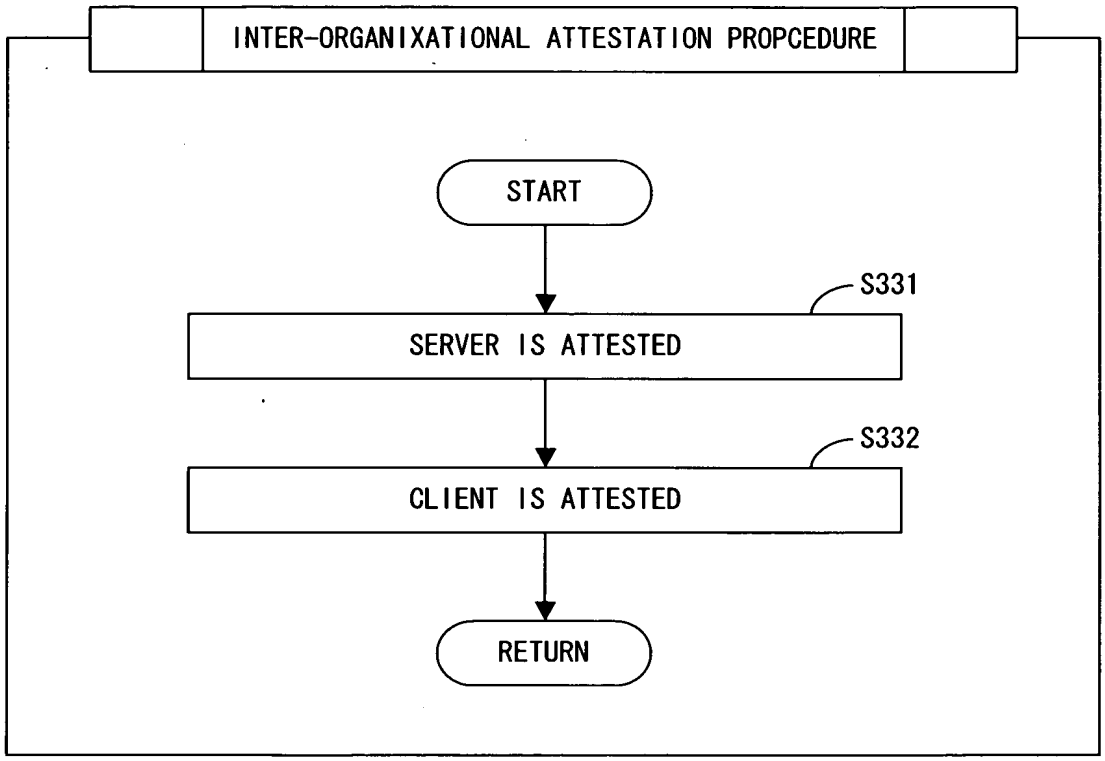
INTER-ORGANIXATIONAL ATTESTATION PROPCEDURE
START
S331
SERVER IS ATTESTED
S332
CLIENT IS ATTESTED
RETURN

FIG. 12

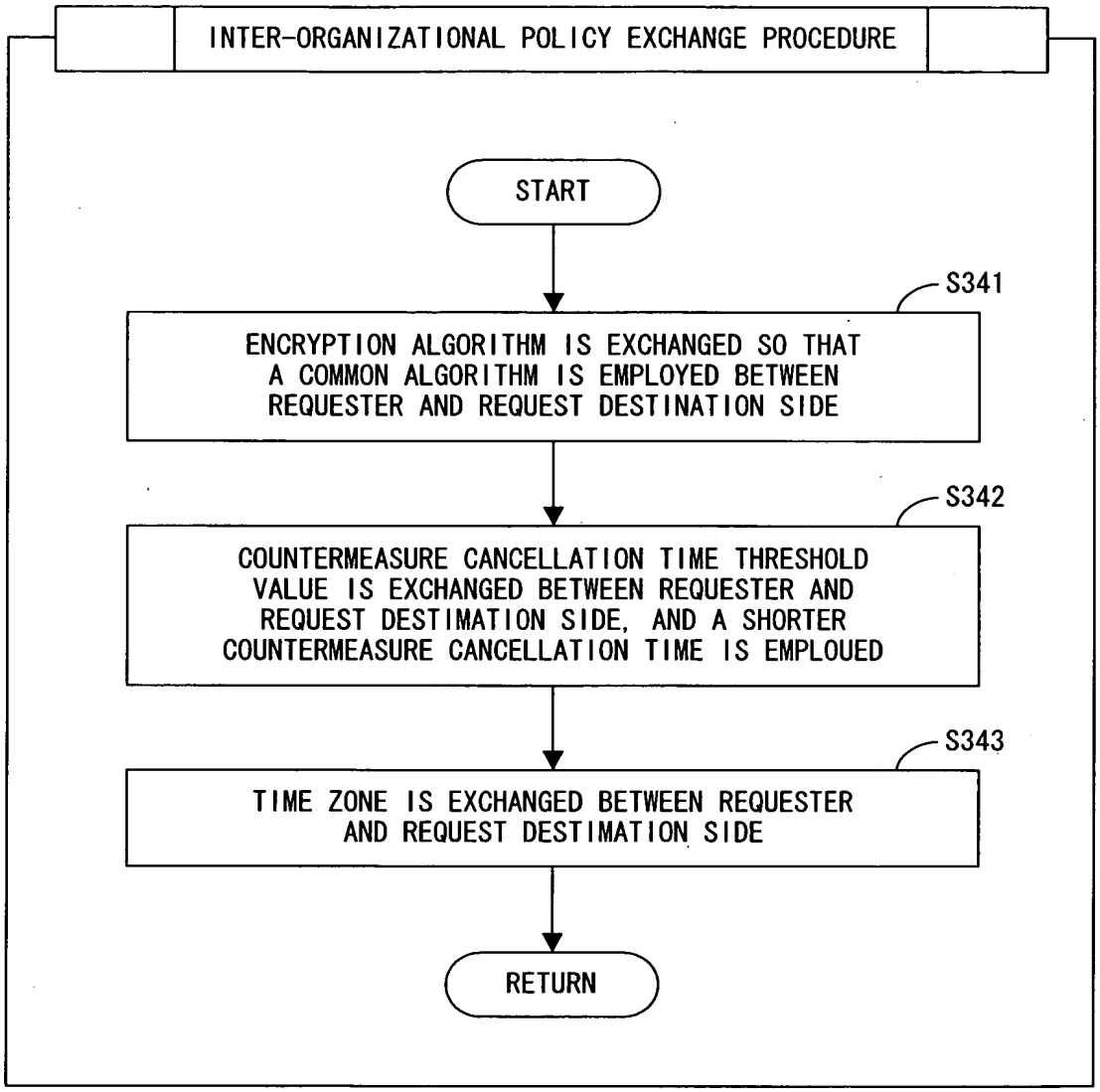
INTER-ORGANIZATIONAL POLICY EXCHANGE PROCEDURE
START
S341
ENCRYPTION ALGORITHM IS EXCHANGED SO THAT A COMMON ALGORITHM IS EMPLOYED BETWEEN REQUESTER AND REQUEST DESTINATION SIDE
S342
COUNTERMEASURE CANCELLATION TIME THRESHOLD VALUE IS EXCHANGED BETWEEN REQUESTER AND REQUEST DESTIMATION SIDE, AND A SHORTER COUNTERMEASURE CANCELLATION TIME IS EMPLOUED
S343
TIME ZONE IS EXCHANGED BETWEEN REQUESTER AND REQUEST DESTIMATION SIDE
RETURN

FIG. 13

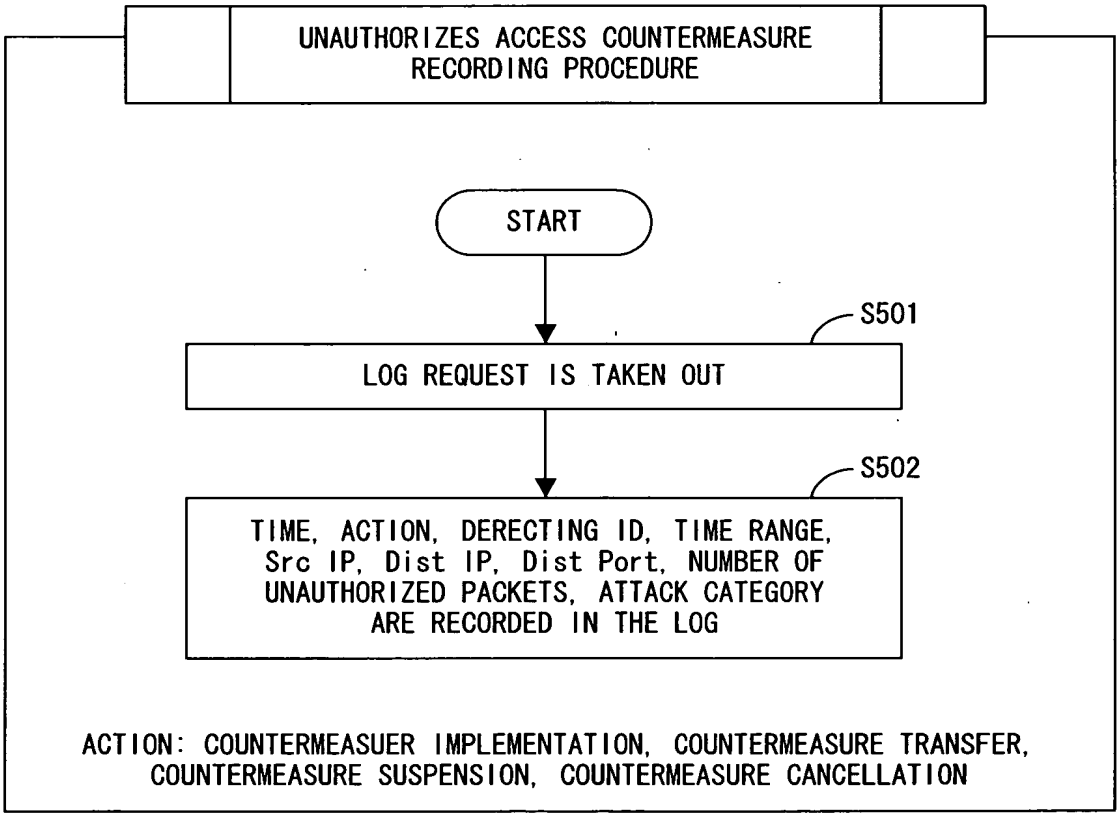
UNAUTHORIZES ACCESS COUNTERMEASURE RECORDING PROCEDURE
START
S501
LOG REQUEST IS TAKEN OUT
S502
TIME, ACTION, DERECTING ID, TIME RANGE, Src IP, Dist IP, Dist Port, NUMBER OF UNAUTHORIZED PACKETS, ATTACK CATEGORY ARE RECORDED IN THE LOG
ACTION: COUNTERMEASUER IMPLEMENTATION, COUNTERMEASURE TRANSFER, COUNTERMEASURE SUSPENSION, COUNTERMEASURE CANCELLATION

FIG. 14

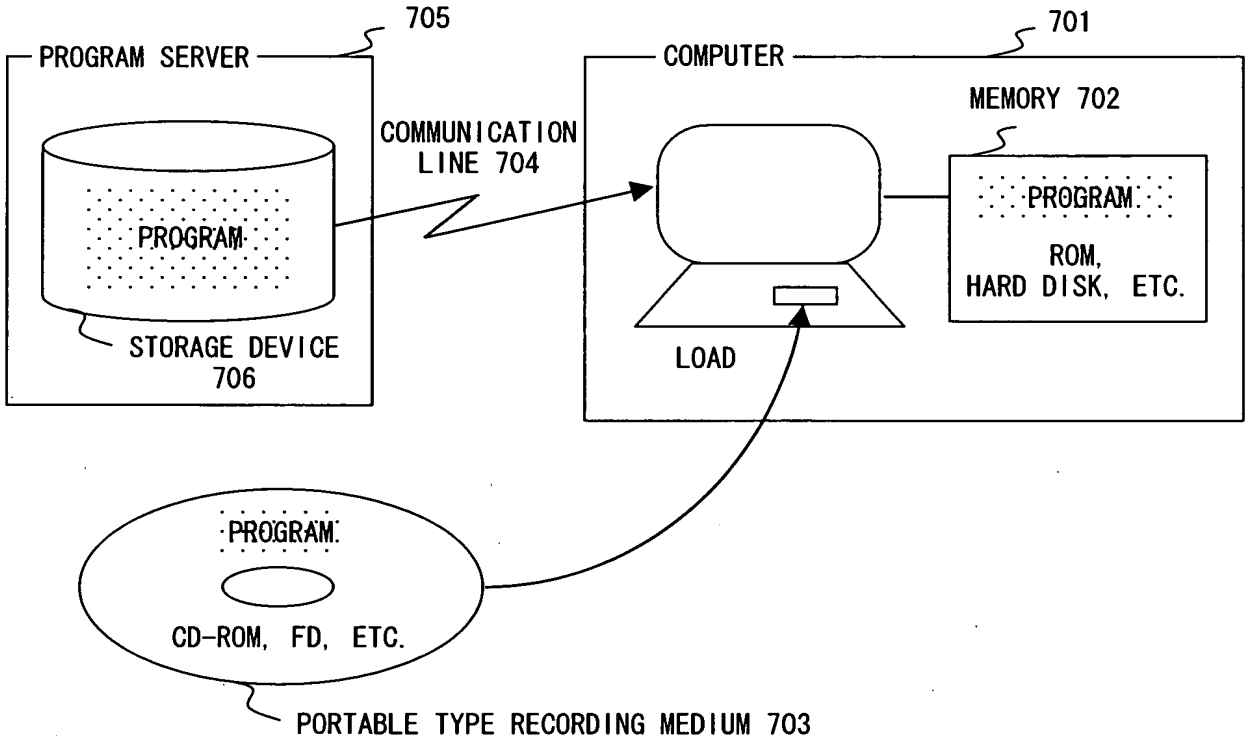
705
PROGRAM SERVER
PROGRAM
STORAGE DEVICE
706
COMMUNICATION
LINE 704
701
COMPUTER
MEMORY 702
PROGRAM
ROM,
HARD DISK, ETC.
LOAD
PROGRAM
CD-ROM, FD, ETC.
PORTABLE TYPE RECORDING MEDIUM 703

FIG. 15